ISC – Information Resources Policies

Table of Contents

POLICY 1.00: DATA SECURITY **2**
POLICY 2.00: RESERVED FOR FUTURE USE **4**
POLICY 3.00: RESERVED FOR FUTURE USE **5**
POLICY 4.00: RESERVED FOR FUTURE USE **6**
POLICY 5.00: INFORMATION SYSTEMS MANAGEMENT & SYSTEM DEVELOPMENT LIFE CYCLE **7**
POLICY 6.00: ARCHITECTURE **9**
POLICY 7.00: INFORMATION SYSTEMS PLANNING **10**
POLICY 8.00: RESERVED FOR FUTURE USE **12**
POLICY 9.00: DISASTER RECOVERY **13**
POLICY 10.00: DATA RESOURCE MANAGEMENT **15**
POLICY 11.00: RESERVED FOR FUTURE USE **17**
POLICY 12.00: OPEN ACCESS TO ELECTRONIC INFORMATION **18**
POLICY 13.00: NETWORK INFRASTRUCTURE SUPPORT AND MAINTENANCE **21**

ISC – Information Resources Policies

Policy 1.00: Data Security

All information technology resources must be appropriately and adequately protected against unauthorized access, modification, destruction or disclosure.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure that all information technology resources are protected in accordance with the statutes of the State of Tennessee.
2. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.
3. Define the responsibilities of information systems management and users in the protection of information technology resources.
4. Provide access to authorized users.

SCOPE:

All information technology resources and associated components, such as networks, telecommunications, hardware, software, data, related documentation, and reports.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Develop the standards, procedures, and guidelines necessary to assure security of the State's information technology resources.
2. Provide technical consulting support to agencies in fulfilling their information technology resources security goals.
3. Provide technical support, training and recommendations for the agencies' use of the State's standard systems security software.
4. Provide ongoing technical reviews of security aids, tools, techniques and other methods to meet security requirements: develop and recommend, in conjunction with agencies, to the Information Systems Council new or revised policies necessary to assure security of the State's information technology resources.
5. Provide for an administrative review of security standards, procedures, and guidelines in light of technical, environmental, procedural or statutory changes which may occur.
6. Protect information technology resources under OIR's control in accordance with statewide policies, standards, and procedures.
7. Assign an individual the responsibility and authority for administrative oversight of security for the State's information technology resources.

ISC – Information Resources Policies

Agency Management, Information Systems Group

1. Assign an individual the responsibility and authority for administrative oversight of security for information technology resources under the agency's control.
2. Establish agency policies, standards, procedures, and guidelines for securing the agency's information technology resources consistent with published statewide directives.
3. Protect information technology resources under agency control in accordance with applicable statutes and with policies, standards, procedures, and guidelines established at both the statewide and agency levels.
4. Educate agency users on security policies, standards, procedures and guidelines related to information technology resources.
5. Provide for an agency administrative review of security standards, procedures and guidelines in light of technical, environmental, procedural, or statutory changes which may occur.

Individual Users

1. Adhere to statewide and agency policies, standards, procedures and guidelines pertaining to information technology resources security.

ISC – Information Resources Policies

Policy 2.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 3.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 4.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 5.00: Information Systems Management & System Development Life Cycle

Information systems projects will follow a standard project management methodology and information systems will be developed using a standard System Development Life Cycle (SDLC).

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Provide a defined project management methodology, which will provide guidance and consistency in the execution of all projects.
2. Provide a common process for status reporting and facilitate quality and funding reviews.
3. Provide a development life cycle methodology, which will define a detailed framework for ensuring the requirements are identified and the solutions are developed and deployed using a standardized process.
4. Deliver quality systems on time and within budget in a consistent and maintainable manner that conforms to the State's software and hardware architectural and security infrastructure standards.

SCOPE:

The policy applies to all (a) statewide and departmental, (b) mainframe and distributed, and (c) in-house developed and procured information system projects and application systems development.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Develop and maintain an Information Technology Methodology (ITM) based on industry best practices that are adapted to the state's needs for a standard project management guide.
2. Develop a System Development Life Cycle (SDLC) methodology that incorporates design and development standards, procedures, guidelines, and best practices in support of the State's architectural standards.
3. Provide the availability of training classes in the use of the methodologies and development processes.

4. Provide consulting support in the use of the methodologies and development processes.
5. Provide access to the ITM and SDLC documentation on the OIR intranet.
6. Provide a base of skilled project managers and developers in support of agencies systems development needs.
7. Incorporate the methodologies and development techniques in all application development projects.

Agency Management

1. Train appropriate agency personnel in the use of the methodologies and techniques.
2. Incorporate the methodologies and development techniques in all application development projects.

ISC – Information Resources Policies

Policy 6.00: Architecture

Standards and guidelines will be established to support a common Information Technology infrastructure that enables the effective use of information technology in the State.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

Office for Information Resources, *Tennessee Information Resources Architecture*.

OBJECTIVES:

1. Ensure a compatible statewide network of information technology hardware, software, and communications resources.
2. Enable the interchange of data.
3. Allow for the cost effective use of information technology systems while maintaining maximum compatibility statewide.
4. Provide standard prerequisite functional requirements for hardware and software procurements.
5. Ensure agency technical direction is in alignment with overall State technology policy.

SCOPE:

The policy applies to all information technology resources.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Establish a process for the review of agency requests for exceptions to the Tennessee Information Resources Architecture.
2. Maintain the *Tennessee Information Resources Architecture*.
3. Establish procedures to support the use of the architecture at the state, departmental, and desktop levels.
4. Establish procedures to ensure that the architecture evolves as technology progresses.

Agency Management

1. Technology direction and objectives must be in alignment with overall State objectives and comply with the Tennessee Information Resources Architecture.
2. Participate in the architectural review process and provide input to the review of components of the architecture.

ISC – Information Resources Policies

Policy 7.00: Information Systems Planning

An Information Systems Plan will be prepared annually by each agency. All agency requests for information technology resources and services will be reviewed. Major technology requests may be presented to the Information Systems Council. The Office for Information Resources will administer the planning and review process and prepare a Statewide plan.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

State of Tennessee Information Systems Planning Guidelines

State of Tennessee Cost Benefit Analysis Methodology

OBJECTIVES:

1. Develop and document the agency's information technology needs, costs and anticipated benefits and savings to the State.
2. Provide a mechanism for identifying future technology needs, and information resource management issues within the State.
3. Identify and prioritize the information technology projects within the agency as a prelude to the budgetary process.
4. Provide for the formal review of information technology requests. Reviews will consider business alignment, feasibility, service level, cost effectiveness and adherence to the State's information technology policies and architectural standards.
5. Identify statewide information technology requirements.
6. Provide information to facilitate the management of information resources within the State.

SCOPE:

This policy applies to all state agencies.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Establish guidelines and procedures by which the plan will be developed.
2. Establish procedures for the review of agency requests for information technology resources and services. The review will consider business alignment, feasibility, cost effectiveness and adherence to the information systems policies and standards.
3. Responsible for the consolidation of the agency plans into a statewide plan.

Date Last Revised – 9/14/2004 – Approved by the Information Systems Council

4. Responsible for the identification of statewide information technology requirements for budgetary planning.
5. Responsible for providing training and guidance to agencies to support the development of their plan.

Agency Management

1. Responsible for developing the agency Information Systems Plan following the guidelines provided.
2. Responsible for updating the plan as needed throughout the year.
3. Establish procedures for the review of agency requests for information technology resources and services by agency management.

ISC – Information Resources Policies

Policy 8.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 9.00: Disaster Recovery

Disaster recovery planning and the capability for implementing a recovery are required encompassing all critical data processing applications and their peripheral support activities.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Ensure that all critical information systems can be recovered in the event of a disaster which disrupts any of the data processing facilities of the State.
2. Provide the capability to continue processing critical information systems, both centralized and departmental, in the event of a disaster.
3. Define the responsibilities of OIR and agency information system management in the development of a disaster recovery plan for critical information systems.

SCOPE:

The policy will apply to all Agency-level and Statewide systems.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Develop and recommend to agencies, the standards, procedures and guidelines necessary to assure recovery capabilities for the State's information systems.
2. Define the procedure for declaring a disaster.
3. Define criteria for an application to be defined as critical.
4. Provide an ongoing technical review of disaster recovery aids, tools, techniques and other methods to meet ongoing disaster recovery requirements.
5. Provide for an administrative review of disaster recovery considerations in light of technical, environmental, procedural or statutory changes which may occur.
6. Provide management and technical consulting support to agencies in fulfilling their disaster recovery roles.
7. Utilize disaster recovery software and create the centralized disaster recovery plan.
8. Provide centralized disaster recovery coordinator and alternate.

Agency Management

1. Responsible for establishing policies and procedures for the development of the agency's disaster recovery plan.

2. Provide an agency disaster recovery coordinator who will be responsible for ensuring that the agency's portion of the centralized plan and that the agency's individual plan allow the agency to recover their critical information systems.
3. Responsible for establishing recovery procedures for the peripheral activities required to continue the agency's critical production tasks.

ISC – Information Resources Policies

Policy 10.00: Data Resource Management

Data is a valuable resource and shall be managed and optimized to benefit the State as a whole.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.

OBJECTIVES:

1. Plan and promote the effective and efficient sharing and usage of data to support State Government.
2. Ensure personnel have access to the data they need to perform their job functions.
3. Promote the understanding and accessibility of the State data resources.
4. Facilitate ad hoc access and reporting of data maintained in relational databases.
5. Ensure data resources will be shared among systems (applications, users, agencies).
6. Ensure data redundancy is minimized and managed.
7. Ensure data will be precisely and consistently defined (i.e. that standards exist and are enforced).
8. Manage the data life cycle independent of the application system life cycle.

SCOPE:

This policy applies to all data utilized at the State.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Implement the facilities, standards, and procedures necessary to document and maintain information about data in a State repository.
2. Develop and implement standards, procedures, and guidelines for the use of database management facilities.
3. Ensure the physical security and protection of data on systems managed by the Office for Information Resources.
4. Implement and maintain the physical storage definitions, standards, and procedures so that the operational efficiency, integrity, and security of databases are maintained; and that development productivity is maximized in accessing the data.
5. Provide ongoing performance monitoring and tuning of State and departmental level relational databases.

6. Provide design review and approval for logical and physical data models delivered in accordance with the appropriate methodology and State standards, procedures, and guidelines.
7. Provide data access support and guidance.
8. Provide tools and techniques necessary to support ad hoc reporting.
9. Ensure the consistency and quality of the State data resources by coordinating the ongoing maintenance of standards, guidelines, and procedures; ensuring that published standards and procedures are followed.
10. Provide training for the use of techniques and facilities related to data analysis and the utilization of State database facilities.

Agency Management

1. Construct agency data models. Provide data analysis deliverables in accordance with the appropriate methodology and State standards, procedures, and guidelines.
2. Provide complete and accurate business descriptions of data elements to maintain the central repository.
3. Ensure the integrity of data maintained in automated files or databases and of reports produced from the data.
4. Ensure the physical security and protection of data on systems managed by the Agency.
5. Develop internal procedures which comply with State data-related standards and guidelines.
6. Assign responsibility for controlling access to agency data resources.

ISC – Information Resources Policies

Policy 11.00: Reserved for Future Use

ISC – Information Resources Policies

Policy 12.00: Open Access to Electronic Information

The State of Tennessee will aggressively and cost-effectively use information technology, as well as emerging technologies, in order to provide efficient, effective, equal, and universal citizen access to public information as defined by law.

REFERENCE:

Tennessee Code Annotated, Sections 10-7-301, 10-7-503, and 10-7-504 -- as amended.

Federal laws, such as the Freedom of Information Act, the Privacy Act, and the Americans with Disabilities Act, which govern the use, disclosure, and accessibility of data collected by government programs which are partially or completely federally funded.

OBJECTIVES:

1. Promote interaction among citizens, governments, businesses and organizations, as well as efficient dissemination of mission-related public information, through the use of information technology.
2. Provide broad, equitable, and affordable access to electronically-stored, non-restricted public records seeking to ensure that all citizens have access to such records. This includes citizens with disabilities, citizens with limited financial resources, and citizens from rural areas.
3. Assure protection of the individual citizen's privacy rights by safeguarding electronically-stored, legally-defined private and confidential information.
4. Maximize the convenience and cost-effectiveness of electronic access to public information through intergovernmental coordination and organization of information.
5. Based upon statutory authorization, establish uniform methods for calculating charges for the creation and provision of online electronic access to public records, as well as for the copying of electronic files containing public records.
6. Provide a coherent and collaborative framework for government agencies to address these objectives.

SCOPE:

All electronically-stored, non-restricted public records housed within the state's information technology environment.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Incorporate in the Information Systems Planning process (see Policy No. 7.00) a component which addresses the electronic dissemination and access of public 0information to Tennessee citizens.
2. Develop a comprehensive and structured identification or classification system (TILS - Tennessee Information Locator System) which provides an effective means for organizing and locating information resources made available for electronic access; thus, in composite form, establishing a state inventory for managing the state's information holdings.
3. Ensure that agency information holdings are identified and described in the state's information inventory, and that information is effectively disseminated.
4. Require that appropriate security controls are in place to protect critical systems and to prohibit access to restricted information by remote electronic means.
5. Guided by statute(s), establish pricing guidelines for creating and providing online electronic access to public records, as well as for copying electronic files containing public records.
6. Provide the infrastructure for remote access to public records via the most widely dispersed and generally available technologies.
7. Promote collaboration among government agencies to provide citizens with access to "related" public records. Through the "bundling" of these records, OIR will seek to avoid duplication of information, to make access to information more convenient for citizens, and to share the cost of technology.

Agency Management, Information Systems Group

1. Provide access to electronically-stored, non-restricted government information. While online public access may not be feasible for existing information systems, agencies must plan for such capacity in the design of future systems and information dissemination strategies.
2. Confer with the appropriate agency officials to identify the types of electronic public records and public record information under their custody which are exempt from inspection, examination, and copying under Tennessee's Open Records Law or other legislation.
3. Assess and define electronic dissemination and access needs, together with the information systems required to respond to those needs, for any new systems at an early stage of the project planning process.
4. Be knowledgeable of all electronic public access activities that involve the agency's data.
5. Provide adequate staff training in the requirements of Tennessee's Open Records Laws and the responsibilities set forth in this policy, with particular attention to staff's responsibility for maintaining the confidentiality of exempt information or records.
6. Ensure that all electronic data subject to restricted access (in accordance with Tennessee's Open Records laws and other applicable statutes or regulations which authorize such restriction) are properly identified and managed.

7. Assure that all data provided for electronic dissemination and access to the public are kept up-to-date and accurate.
8. Provide timely updates to the state's inventory of information resources. The provisioning of public records via information technology must be compliant with the Tennessee Information Locator System (TILS) Guidelines to ensure the widest possible access to these records.
9. Minimize repetition and duplication of electronically disseminated information by utilizing the state's information inventory.
10. Adhere to established guidelines and statutes concerning the calculation of charges for the creation and provision of online electronic access to public records, as well as for the copying of electronic files.
11. Publicize that public information can be accessed via technology.

ISC – Information Resources Policies

Policy 13.00: Network Infrastructure Support and Maintenance

The Office for Information Resources will manage and secure the State's network infrastructure to ensure the reliability, integrity, availability, and confidentiality of the operations of government and those it serves.

REFERENCE:

Tennessee Code Annotated § *4-3-5501,* effective May 10, 1994 [Acts 1994, ch. 992, § 2; 1995, ch. 305, § 66]
Tennessee Code Annotated § *4-3-5502,* effective May 10, 1994 [Acts 1994, ch. 992, § 3.]
Tennessee Code Annotated § *4-3-5503,* effective May 10, 1994 [Acts 1994, ch. 992, § 4.]

OBJECTIVES:

1. Ensure continuous efforts to secure information systems authorized by the "National Strategy to Secure Cyberspace" initiative of the United States and the President's Executive Order 13231 of October 2001.
2. Ensure connectivity for state agency systems and access to data maintained by all state departments, agencies, commissions, or boards.
3. Protect the networks serving, and the data concerning, the citizens of the State of Tennessee from unauthorized access, disruption, and/or corruption, and ensure efficiencies and network availability.
4. Ensure the security and privacy of protected health information mandated by federal law under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
5. Ensure improved network efficiencies, availability and security.
6. Ensure enhanced security by the establishment and enforcement of standards and standard desktop configurations.
7. Implement a fully developed statewide security policy to protect the security and privacy of the State's data and the operations of government and those it serves.
8. Ensure the efficiencies offered by single State agency management of the security of network related system are maximized, under the Office for Information Resources (OIR) of the Department of Finance and Administration as it is best positioned, equipped and authorized to perform these functions.
9. Promote efficiencies to ensure the existing rate structure for Local Area Network (LAN) and Wide Area Network (WAN) nodal fees provide sufficient capacity to implement this policy.

ISC – Information Resources Policies

SCOPE:

This network infrastructure support and maintenance policy includes all information technology resources and associated network infrastructure components, including the strategies, policies, standards, procedures, and guidelines necessary to assure security of the State's information technology resources, as well as all distributive processing and network related systems; and to serve as a computer service bureau.

IMPLEMENTATION:

Department of Finance & Administration, Office for Information Resources

1. Responsible for and authorized to manage and secure the State's networks.
2. Ensured physical access to those areas where network infrastructure is maintained including all circuits, firewalls, intrusion detection systems, and other enterprise network defense systems required to provide connectivity and to manage and/or secure the State's networks and data.
3. Authorized to establish and enforce policy and statewide standards for security, network and internet access, servers (application servers, DNS servers, web servers, etc.) wired or wireless technology, e-mail, web sites, network monitoring, computer technology standards, firewall policy, intrusion detection, authentication, availability of resources, network maintenance, and for handling violations and security incidents for state owned or supported networks.
4. Responsible for identifying or developing guidelines covering cyber awareness literacy, training, and education, including ethical conduct in cyberspace.
5. Responsible for providing the secure, centralized, and standardized management of Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs) including policies and connectivity to enhance the implementation and management of security and thereby reduce time lost to recover from security intrusions, viruses, and "hackers."
6. Responsible for securing the network through the effective and efficient application of resources to make satisfactory network repairs; and should detachment occur, responsible to communicate immediately with the agency to advise it of findings, cause for detachment, and commit resources to work with the agency to assist in satisfactory repair.
7. Provide assistance to and partner with agencies in the creation of guidelines, procedures, training, and tools in order for agencies to conduct self-monitoring and self-assessment.
8. Responsible for and authorized to perform audits on any device that attaches to the State of Tennessee's network or affects cyber security.
9. The State's Chief Information Officer, as a member of the State's Homeland Security Council, is authorized to act in the best interest of the State to assign network priorities in the event of either a homeland security incident, or the catastrophic loss of core network processing capability, and will ensure appropriate dialogue with the Homeland Security Council leadership.

ISC – Information Resources Policies

Agencies and Other Attached Entities

1. Each department, agency, commission, board, local governmental entity, or state supported institution that attaches to the networks managed by OIR shall adhere to all applicable security and disaster recovery policies, standards, and procedures for the State's information systems environment and shall sign a Network Connectivity Agreement with OIR.
2. Information systems security coordinators shall be appointed as department, agency, commission, board, or institution representatives; and, shall be responsible for information systems security coordination as specified in the agency Network Connectivity Agreement.
3. Each department, agency, commission, and board that attaches to the networks managed by OIR shall adhere to standards for server configuration and shall have the configuration reviewed and approved by OIR prior to attaching the server to a network segment, and shall submit to no-notice annual OIR performed audits.
4. Each vendor, subrecipient, or contracting company and their employees doing business with the State and that attaches to OIR managed networks shall adhere to all applicable security and disaster recovery policies, standards, and procedures for the State's information systems environment and shall sign a Network Connectivity Agreement with the OIR.
5. Each department, agency, commission, and board that issues network or system user IDs to employees, contractors, vendors or subrecipients shall obtain a signed State of Tennessee Acceptable Use Policy Network Access rights and Obligations User Agreement Acknowledgement from each employee, contractor, vendor or subrecipient as a condition of ID issuance**.**

Exclusions and Exemptions

1. This policy excludes Ultra High Frequency (UHF), Very High Frequency (VHF), 700 MegaHertz radio, and 800 MegaHertz radio ranges, and data wireless communication systems involving law enforcement officers and first responders; car to officer communications, with the exception of wireless Local Area Networks (LANs, 802.11x) that are included within this policy.
2. Non-executive branch agencies, including the Tennessee Bureau of Investigation, the General Assembly, the Judicial Branch, and all Constitutional Officers shall be exempted only from the governance structure defined in this ISC Policy. Exempted entities will maintain similarly stringent network operating system environments to retain full network access privileges, and their procedures, checklists, and performance reports will be reviewed upon request by the Information Systems Council or its designee. The Comptroller's Office will be the Information Systems Council's designee for the General Assembly.